Expanded E- Government

Tom Pyke
Chief Information Officer

The Chief Information Officer is responsible for implementing the e-Government initiative of President George W. Bush's management agenda at DOE. This initiative drives improved information technology management, elimination of redundant processes, and increased cyber security. In the last four years, the Department has made tremendous progress in e-Government.

DOE has improved information technology management by reenergizing the Information Technology Council that is responsible for reviewing IT investment business cases, overseeing project performance and ensuring the remediation of poorly performing projects. We also developed a comprehensive IT project managers' certification program to ensure vigorous project management, and documented and implemented earned value management policy and procedures for IT projects to reduce risk and improve project performance. By establishing an Enterprise Architecture that aligns to the Federal Enterprise Architecture, we have ensured that all Department IT investments follow our Modernization Roadmap. We have supported the reduction of redundant processes government-wide by participating in 18 of the President's 24 e-Government initiatives, E-Authentication, and the six Lines of Business established by the Office of Management and Budget. In addition, we identified fifteen candidates to leverage e-Government opportunities within the Department and have initiated or completed thirteen of the fifteen with the remaining two scheduled for implementation within the next two years. We have increased the security of our IT enterprise by certifying and accrediting more than 97% of our information systems. We have updated and augmented our cyber security policies and are now institutionalizing them, to include incident reporting and cyber security related to wireless technology use.

The e-Government team at the Department of Energy has laid the foundation necessary to meet the requirements of the PMA. Our vision for the future is to build on that foundation and make DOE the best-managed Department in the Federal Government.

Highlights of What We've Accomplished

- *Established Process to Monitor Information Technology (IT) Project Development Performance*. All major IT projects are reviewed quarterly to ensure that cost and schedule overruns, and performance shortfalls average less than 10 percent against approved baselines.

- *Established a Rigorous Process to Review Proposed IT Projects.* IT projects over $5 million are identified as major investments and are subject to a rigorous review process. The process requires review and approval recommendations from the Office of the Chief Information Officer/IT Council and Departmental senior management approval during the Corporate Review Budget phase of the annual budget formulation process.-

- *Established an Earned Value Management (EVM) Policy and Oversight Process.* The Department established EVM policy and guidance and designated a project office to oversee the implementation and certification of EVM for major IT investments. All required major IT projects report EVM performance monthly and overall performance is reported to the Secretary and Deputy Secretary quarterly.

- *Established Governance Review Process for Enterprise Architecture Artifacts and Investment Alignment.* Governance includes establishment of an Architecture Review Board and coordination with the IT Council to review and recommend approval of EA artifacts and the alignment of IT investments with the architecture. IT projects are reviewed to ensure that they map to the Department's enterprise architecture and the Federal Enterprise Architecture. Previously, no such rigor existed resulting in a lack of standardization and poorly managed systems.

- *No DOE IT Business Cases appear on the OMB Watch List.* To date, DOE has successfully removed all major IT business cases from the OMB Watch List for BY 2006 ahead of the deadline. The Watch List includes IT investments that OMB has determined do not have an adequate business case and therefore need corrective actions and remediation.

- *Cyber Security Incident Reporting – Over 98% of DOE Sites Reporting.* Incident reporting helps the Department and other federal agencies identify and quickly remediate cyber security vulnerabilities in the enterprise. Cyber security incidents are reported monthly to the Computer Incident Advisory Capability (CIAC) team, and summary reporting performance of security incidents is provided to the Secretary and Deputy Secretary quarterly.

- *Certified and Accredited the Security of over 97% of all Reported Information Systems.* The Office of the CIO meets with Program Offices quarterly to review progress on implementation of cyber security requirements including certification and accreditation (C&A), thus ensuring the systems help provide DOE quality products.

- *Implemented a Departmental Independent Verification and Validation (IV&V) process.* This process ensures that cyber security requirements are implemented consistently across the complex. The IV&V team reviews C&A documentation from all Program Offices and provides advice and assistance to those offices determined to be deficient. Also, Site Assistance Visits are conducted at various field sites to ensure robust cyber security complex-wide**.**

- *Established a Homeland Security Presidential Directive 12 (HSPD-12) Project Team.* This team is taking a systemic engineering approach to provide a common, government-wide identification standard for all Federal and applicable Contractor personnel at DOE**.**

- *Established a Homeland Security Presidential Directive 7 (HSPD-7) Inter-Departmental Steering Group.* This Group and its committees are coordinating the Department's effort to identify, prioritize and protect the Department's critical infrastructure and key resources as outlined in the Presidential directive.

- *Established the Cyber Security Executive Steering Committee.* This Committee is a joint effort by the Office of the CIO and the National Nuclear Security Administration, to provide advice and oversight for the cyber security program in the Department of Energy. The Committee's goal is to reduce vulnerabilities across the DOE complex through a common, shared appreciation of the importance and challenges of cyber security in the enterprise.

- *Convened Annual Cyber Security Group Training Conference.* This outreach effort promoted awareness and featured training and information sharing dedicated to reducing cyber security vulnerabilities. This annual training was held in Denver, Colorado on April 2005 and was the most well attended conference thus far.

- *Developed and Promulgated the Policy Memorandum to Address Cyber Security Improvements Across the Department of Energy Enterprise.* The CIO and the National Nuclear Security Administration signed a joint memorandum on March 10, 2005, establishing the agency requirements for minimum security configurations and contingency planning. The memorandum also clarifies the requirements for C&A, introduces the Department's next steps for cyber asset management, and promotes security awareness for portable electronic devices while on travel.

- *Improved the Management of DOE IT Infrastructure through Completion of initial Business Cases for the Optimization/Modernization of the Department's Networking and Application Hosting Infrastructure*. Business cases were developed in support of the Department's information technology consolidation effort and represent over $300 million dollars worth of investments in networking equipment, computer software/hardware and related personnel support.

FY 2006 Goals

- *Information System Asset and Boundary Identification.* The Department will implement the first phase of the use of automated tools for identifying information system assets and network boundaries to ensure the agency has a demonstrable process for maintaining a 100% information systems inventory.

- *Revitalize the Cyber Security Program.* Continually enhance the program to include an evolving threat environment to ensure all aspects of Cyber Security Program are implemented to respond adequately to the threat environment.

- *Begin Deployment and Institute an Enterprise-wide Supporting Infrastructure for HSPD-12.* The Department will implement the first phase of the technical infrastructure necessary to issue new digital identity cards.

- *Employ Continuous Testing and Vulnerability Scanning to Validate the Adequacy of Management, Operational and Technical Controls for Cyber Security.* The goal is to provide an enterprise solution for all agency sites.

- *Integrate the Enterprise Architecture Data into the Department's Strategic Planning, Capital Planning, and Budget Formulation Processes.* DOE will develop activities, procedures, and target and transition enterprise architecture artifacts to enhance planning processes Department-wide.

- *Establish and commence deployment of enterprise licensing across the DOE operating environment in support of the "Smart Buy" Program.* DOE will commence the conversion of its Departmental enterprise licensing agreements to the Smart Buy program.